



SPAWAR
Systems Center
San Diego

TECHNICAL DOCUMENT 3099
February 2000

Guidelines for Information Protection under Work for Industry Agreements

Information Protection Plan

Approved for public release;
distribution is unlimited.

SSC San Diego

DTIC QUALITY INSPECTED 4

20000802 227

TECHNICAL DOCUMENT 3099

February 2000

Guidelines for Information Protection under Work for Industry Agreements Information Protection Plan

Approved for public release;
distribution is unlimited.



SSC San Diego
San Diego, CA 92152-5001

SSC SAN DIEGO
San Diego, California 92152-5001

E. L. Valdes, CAPT, USN
Commanding Officer

R. C. Kolb
Executive Director

ADMINISTRATIVE INFORMATION

This document was produced with in-house funding to provide guidance and process descriptions for SSC San Diego personnel who work to ensure acquisition integrity whenever SSC San Diego enters into agreements with Industry pursuant to Title 10 U.S. Code, Sections 2371, 2539b, and 2553 and Title 15 U.S. Code, Section 3710a.

Released under authority of
S. E. Miller
Office of Counsel


FOREWORD


These Guidelines for Information Protection under Work for Industry Agreements provide guidance and process descriptions for Space and Naval Warfare Systems Center, San Diego (SSC San Diego) personnel supporting Industry. Our objective is to define procedures for protecting and handling competition-sensitive, company-proprietary, and source-selection information. Adherence to these guidelines and processes will ensure acquisition integrity whenever SSC San Diego enters into agreements with Industry pursuant to Title 10 U.S. Code, Sections 2371, 2539b, and 2553 and Title 15 U.S. Code, Section 3710a.

This document formalizes policies that have been in place since SSC San Diego signed its first agreement with Industry in December 1998.

Reviewed and Concurred by:



DR. TOM KAYE
Deputy Executive Director
Science, Technology & Engineering



MR. SCOTT E. MILLER
Counsel
Office of Counsel


CDR BRUCE E. GREEN, USN
Head
Supply and Contracts Department


MR. RICHARD A. FLETCHER
Head
Security Office


for MR. ROBERT L. FRYE
Comptroller


DR. ROBERT C. KOLB
Executive Director

Approved by:

CAPT ERNEST L. VALDES, USN
Commanding Officer
SSC San Diego

CONTENTS

| | |
|---|------------|
| FOREWORD..... | iii |
| 1. INTRODUCTION..... | 1 |
| 1.1 BACKGROUND..... | 1 |
| 1.2 PURPOSE..... | 1 |
| 2. ACQUISITION INTEGRITY—ORGANIZATIONAL FIREWALLS..... | 2 |
| 2.1 SSC SAN DIEGO INDUSTRY SUPPORT TEAM INFORMATION PROTECTION PLAN..... | 2 |
| 2.2 FIREWALL DEFINITION | 2 |
| 2.3 FIREWALL GUIDELINES | 2 |
| 2.4 PROCESSES | 3 |
| 2.4.1 Guidance | 3 |
| 2.4.2 Non-Disclosure Agreements (NDAs)..... | 3 |
| 2.4.3 Competition-Sensitive, Company-Proprietary, or Source-Selection Information | 7 |
| 2.4.4 Requests for BOK Information or Support..... | 7 |
| 2.4.5 Termination of Team Membership or Team Support | 10 |
| 3. ROLES AND RESPONSIBILITIES | 12 |
| 3.1 BUSINESS DEVELOPMENT OFFICE INDUSTRY LIAISON POINT OF CONTACT . | 12 |
| 3.2 OFFICE OF COUNSEL | 12 |
| 3.3 CONTRACTS | 13 |
| 3.4 SECURITY | 13 |
| 3.5 SSC SAN DIEGO INDUSTRY SUPPORT TEAM LEADERS | 13 |
| 3.6 INDUSTRY SUPPORT TEAM MEMBER..... | 14 |
| 3.7 BODY OF KNOWLEDGE MEMBERS..... | 14 |
| 3.8 PROGRAM OFFICE SUPPORT TEAM MEMBERS | 14 |
| 4. SECURITY | 15 |
| 4.1 COVER SHEETS | 15 |
| 4.2 MAGNETIC MEDIA LABELS | 15 |
| 4.3 BADGES FOR SSC SAN DIEGO IST MEMBERS | 15 |
| 4.4 INFORMATION SECURITY..... | 15 |
| 4.5 CLASSIFICATION MANAGEMENT | 16 |
| 4.6 PHYSICAL SECURITY | 16 |
| 4.6.1 Physical Security Procedures..... | 16 |
| 4.6.2 Vehicle Inspection..... | 16 |
| 4.7 VISIT AUTHORIZATION LETTER | 16 |
| 4.8 DESTRUCTION OF MATERIAL | 17 |

| | |
|--|-----------|
| 5. CONTACT WITH PARTIES OTHER THAN THE INDUSTRY CONCERN WITH WHICH SSC SAN DIEGO IS WORKING | 19 |
| 5.1 PROCEDURES | 19 |

APPENDICES

| | |
|-------------------------------|-----|
| APPENDIX A: DEFINITIONS | A-1 |
| APPENDIX B: ATTACHMENTS | B-1 |

Figures

| | |
|--|----|
| 1. Basic firewall structure..... | 3 |
| 2. Non-Disclosure Agreement for an Individual Assigned to a Particular IST | 5 |
| 3. Non-Disclosure Agreement for a Body of Knowledge (BOK) Member..... | 6 |
| 4. Request for Body of Knowledge Information or Support | 8 |
| 5. Exit Briefing for Termination of Team Membership or Support..... | 11 |

Table

| | |
|---------------------------|---|
| 1. Points of contact..... | 3 |
|---------------------------|---|

1. INTRODUCTION

1.1 BACKGROUND

Recent acquisition reform initiatives are enabling Industry to assume primary responsibility for performing all aspects of the design and construction of major new platforms, including DD 21 and CVN 77. Reconsideration of traditional roles and relationships between Government and the private sector in the context of current and future ship-acquisition programs is required. Concurrently, significant new statutory regulations have been enacted for the purpose of encouraging sales of Government articles, services, and information to non-Department of Defense customers.

In September 1998, the Space and Naval Warfare Systems Command (SPAWAR) and the Program Executive Office (PEO) for DD 21 entered into a Memorandum of Agreement that defines the role of SPAWAR claimancy activities for providing products and services to Industry participating in the DD 21 program. The objective of this Memorandum of Agreement is to facilitate sharing the substantial national investment in technology at SPAWAR with these DD 21 Industry concerns. Within this framework, the Space and Naval Warfare Systems Center, San Diego (SSC San Diego) has negotiated and is currently participating in multiple agreements with Industry concerns that are the prime contractors for DD 21 and other major new combatant platform programs.

1.2 PURPOSE

This document is the principal tool for implementing guidelines and procedures for protecting information when entering into agreements with Industry.

The objective is to ensure acquisition integrity for these SSC San Diego agreements. In the context of work for Industry agreements, the Government is the Seller and Industry is the Purchaser. For purposes of this document, the term "Industry" refers to the entity that is purchasing Government services, referred to as the "Purchaser" in the "Sale of Articles or Services Agreement." SSC San Diego personnel supporting Industry will be referred to as the "Industry Support Team" or "IST"; any reference to competition-sensitive, company-proprietary, and source-selection information to be protected will be simply termed "the information."

Matters pertaining to patent issues and rights in intellectual property, data, mask works, and inventions are addressed in the agreement between SSC San Diego and Industry.

2. ACQUISITION INTEGRITY—ORGANIZATIONAL FIREWALLS

Successfully meeting Program objectives demands a comprehensive plan to ensure acquisition integrity of the competing Industry concerns. Equal treatment involves protection of information, access to relevant information, and free and open exchange of non-competition-sensitive information. The approach described in this section is designed to create a secure and flexible environment. Establishing and maintaining the integrity of the acquisition process is of fundamental importance.

2.1 SSC SAN DIEGO INDUSTRY SUPPORT TEAM INFORMATION PROTECTION PLAN

This document, “Guidelines for Information Protection under Work for Industry Agreements” (the Information Protection Plan), documents SSC San Diego’s role in supporting a secure, competitive business environment. This section of the document provides guidelines for and defines the firewall process as implemented at SSC San Diego. All Work for Industry projects will be governed by this document and a Standard Operating Procedure (SOP) specific to the type of agreement implemented with addenda, if necessary, outlining any unique requirements of an individual program.

2.2 FIREWALL DEFINITION

A firewall is defined as an administrative or physical separation of employees and information to prevent inappropriate disclosure or exchange of competition-sensitive, company-proprietary, or source-selection information.

Firewalls are used to protect all forms of media containing information deserving protection including written materials, viewgraphs, video, data, etc., as well as information available electronically via, for example, Industry’s Interactive Data Environment (IDE). Materials used for technical briefings or demonstrations, detailed descriptions of technical tasking or any items marked as competition-sensitive or company-proprietary, or source-selection are examples of items to be protected via firewalls.

2.3 FIREWALL GUIDELINES

As illustrated in figure 1, firewalls pertain to SSC San Diego employees who are functioning in any of the following capacities:

- ☐ As an Industry Support Team (IST) member
- ☐ As a Program Office Support Team (POST) member
- ☐ As a Body of Knowledge (BOK) member executing tasking in support of an IST or a POST member

Definitions of the information-protection responsibilities of SSC San Diego employees who are designated as IST, POST, or BOK members are provided in section 3.

The basic firewall structure shown in figure 1 indicates the need for firewalls to separate: (1) IST members supporting one Industry concern from IST members supporting a competing Industry concern’s efforts; and (2) IST, BOK, and POST members. An Industry Liaison Support Environment is illustrated to ensure that all interactions with Industry are properly executed.

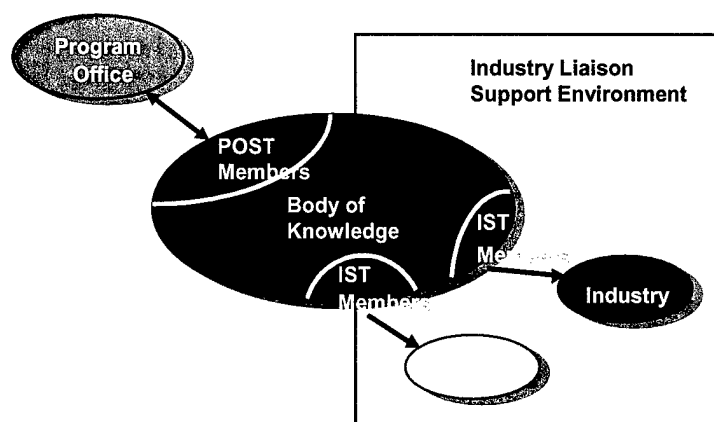


Figure 1. Basic firewall structure.

The following are specific guidelines for SSC San Diego employees working within firewalls.

- ❑ IST members supporting each competing Industry concern working toward the same contract award cannot discuss or otherwise communicate competition-sensitive, company-proprietary, or source-selection information about their IST work with a member of another IST.
- ❑ The content of IST meetings and other activities must be protected with appropriate firewalls.
- ❑ Interactions between IST and BOK members are to be accomplished in accordance with the specific SOP.

2.4 PROCESSES

2.4.1 Guidance

Issues and questions regarding the guidelines set forth in this document shall be addressed in the following way: IST members should direct any issues or questions to their IST Leader (the IST member designated as the technical point of contact for the program); the IST leader should primarily address any issues with the Industry Liaison Point of Contact (ILPOC); BOK members should clarify any concerns with the task leader initiating the task. Should additional guidance be necessary, refer to the Points of Contact listed in table 1 for IST questions regarding this guidance.

Table 1. Points of contact.

| Name | Affiliation | Voice Contact | E-mail | Fax |
|---------------|----------------|----------------|--|----------------|
| Roese, J. | ILPOC | (619) 553-1166 | roese@spawar.navy.mil | (619) 553-3021 |
| Simmons, J. | ILPOC | (619) 553-0257 | simmons@spawar.navy.mil | (619) 553-3021 |
| Miller, S. | Counsel | (619) 553-4703 | millerse@spawar.navy.mil | (619) 553-6656 |
| Fendelman, H. | Patent Counsel | (619) 553-3001 | fendelma@spawar.navy.mil | (619) 553-3821 |
| Esaias, F. | Contracts | (619) 553-4537 | faye@spawar.navy.mil | (619) 553-4464 |
| Talley, P | Security | (619) 553-3195 | patti@spawar.navy.mil | (619) 553-3207 |

2.4.2 Non-Disclosure Agreements (NDAs)

A Non-Disclosure Agreement (NDA) is an agreement by the employee to protect competition-sensitive, company-proprietary, or source-selection information from disclosure to unauthorized personnel (see Appendix A for definitions). The party receiving information from another signs the NDA and agrees not to disclose the information.

All SSC San Diego employees and employees of other agencies supporting an SSC San Diego program shall be briefed about, and acknowledge by signature, the receipt of information on the need to protect one competing Industry concern's information from disclosure to the other Industry concern. The briefing shall address the importance of maintaining information integrity and instruct the incumbent to adhere to the guidelines presented in this section. The ILPOC and the IST Leaders will be responsible for ensuring these guidelines are followed.

An SSC San Diego employee may receive discipline for any violations of the NDA.

Figure 2 is a sample NDA for an individual assigned to a particular IST. Figure 3 is a sample NDA for an individual within the BOK.

NON-DISCLOSURE AGREEMENT FOR AN INDIVIDUAL ASSIGNED TO A PARTICULAR INDUSTRY SUPPORT TEAM (IST)

I understand that in connection with my employment I may acquire or have access to competition-sensitive or proprietary information from an Industry concern participating in the _____ program. I also understand the disclosure of such information to unauthorized persons, either in Industry or the Government, may constitute a violation of procurement statutes and regulations and could jeopardize the integrity of the source-selection process.

I therefore agree to maintain competition-sensitive and company-proprietary information in confidence and to limit disclosure thereof only to authorized persons. In case of doubt, I will obtain advice of local counsel before making such disclosure. (Contact SSC San Diego Office of Counsel, (619) 553-4703.) I will ensure all competition-sensitive or company-proprietary information is properly protected. I agree that this obligation shall continue both during the period of my current employment and thereafter. I also agree to wear a special identification badge developed for Industry Support Team (IST) members at all times while a member of an IST so that someone can identify me as a member of a specific IST.

I agree to remove myself from situations that could lead to disclosure of information from a competing Industry concern.

I understand that as a member of an IST, I have responsibilities that include, but are not limited to, the following:

- ☐ Only support one of the Industry concerns on a particular program and only have access to that entity's information at any one time.
- ☐ Protect that Industry concern's information pursuant to the Guidelines for Information Protection under Work for Industry Agreements.
- ☐ In no way be an advocate for the Industry concern (in meetings, briefings, etc.) or present the Industry concern's design to individuals or organizations outside of that Industry organization.
- ☐ Not have access to any source-selection information on the particular program in which I am working.
- ☐ Make a good faith effort to minimize the number of people having access to protected information.
- ☐ In any interface with either the Program Office Support Team (POST) or with the SSC San Diego Body of Knowledge (BOK), follow all procedures outlined in the Guidelines for Information Protection under Work for Industry Agreements and the appropriate Standard Operating Procedures.
- ☐ Make my IST Leader aware of any disclosures made by myself or someone else and, if appropriate, notify the Office of Counsel for guidance.

I have received a copy of the Guidelines for Information Protection under Work for Industry Agreements, acknowledge that I have read, agree with, and fully understand my obligations therein, and will comply with such obligations.

I understand that violation of this Agreement could result in disciplinary action, up to and including removal. Furthermore, I understand that a violation of this Agreement may result in criminal penalties including fine and/or imprisonment.

Printed Name

Signature

Date

Figure 2. Non-Disclosure Agreement for an Individual Assigned to a Particular IST.

NON-DISCLOSURE AGREEMENT FOR A BODY OF KNOWLEDGE (BOK) MEMBER

I understand that in connection with my employment I may acquire or have access to competition-sensitive or company-proprietary information from or for one or more Industry concerns participating in the _____ program. I also understand the disclosure of such information to unauthorized persons, either in Industry or the Government, may constitute a violation of procurement statutes and regulation and could jeopardize the integrity of the source-selection process.

I therefore agree to maintain competition-sensitive or company-proprietary information in confidence and to limit disclosure thereof only to authorized persons. In case of doubt, I will obtain advice of local counsel before making such disclosure. (Contact SSC San Diego Office of Counsel, (619) 553-4703.) I agree that this obligation shall continue both during the period of my current employment and thereafter.

Competition-sensitive and company-proprietary information includes but is not limited to competing Industry concern's proposals, proprietary information, and reports of a financial, technical, and/or scientific nature regardless of the format and/or medium in which the information is received.

I understand that as a Body of Knowledge (BOK) member, I have the following responsibilities:

- ☐ Ensure that my work is firewalled to protect acquisition integrity and protect against disclosure of protected information.
- ☐ Use results generated in responding to an Industry request strictly for the original demand. The same results shall not be used to respond to any other Industry inquiry under the same program.
- ☐ Ensure any information provided to me by one Industry concern is not provided to a competing Industry concern under the same program.
- ☐ Make a good faith effort to minimize the number of people having access to competition-sensitive or company-proprietary information.
- ☐ Make the appropriate Industry Support Team Leader aware of any disclosures made by myself or someone else.

I have received a copy of the Guidelines for Information Protection under Work for Industry Agreements, acknowledge that I have read, fully understand my obligations therein, and will comply with such obligations.

I understand that violation of this Agreement could result in disciplinary action, up to and including removal. Furthermore, I understand that a violation of this Agreement may result in criminal penalties including fine and/or imprisonment.

Printed Name

Signature

Date

Figure 3. Non-Disclosure Agreement for a Body of Knowledge (BOK) Member.

2.4.3 Competition-Sensitive, Company-Proprietary, or Source-Selection Information

Pursuant to the guidance contained in the Work for Industry Sale of Articles or Services Agreements, Industry and SSC San Diego agree to minimize, to the extent practical, the number of people having access to protected information. SSC San Diego employees and employees of contractors supporting SSC San Diego who receive information belonging to a competing Industry concern or its subcontractors shall agree to

- ☐ Limit its further disclosure to only those SSC San Diego personnel having a need for access to the information.
- ☐ Not disclose such information to the other competing Industry concern or a party not authorized to receive the information.
- ☐ Notify the Office of Counsel at (619) 553-4703 if there are any questions concerning information protection.
- ☐ Use information only in the performance of the work pursuant to the Agreement between the Industry concerns and SSC San Diego.
- ☐ Protect information in accordance with SSC San Diego's standard procedures governing the handling of such information. At a minimum, all competition-sensitive information will be retained in separate, appropriately marked file folders. If the information is also classified, SSC San Diego's procedures for marking and storing such information will also be employed.
- ☐ Not discuss protected information in non-secure and/or public areas.
- ☐ Not leave protected information in non-secure unattended offices or conference facilities.
- ☐ Immediately notify the IST Leader or the ILPOC if an Industry concern or SSC San Diego employee receives information that is not appropriately marked pursuant to information-protection guidelines from any Industry concern or its subcontractors, and reasonably believes that such information should be so marked. In any event, it remains Industry's responsibility to ensure that all documents provided to SSC San Diego are properly marked.

2.4.3.1 Trade Secrets Act. Prior to entering into an agreement with Industry and being subject to the restrictions set forth in the appropriate NDA, all Government employees are charged with the responsibility of protecting Industry and the Government's information pursuant to the Trade Secrets Act (18 U.S.C. 1905). Failure to do so can result in significant penalties including discipline, removal, or imprisonment.

2.4.4 Requests for BOK Information or Support

In those instances where an exchange of technical information between IST or POST members and BOK members is required to accomplish Industry tasking, the individual making the request should ensure that the request is authorized by the appropriate IST or POST leader and that the request is as narrowly focused as is practical. The recommended procedure for performing information exchanges is to document the request for BOK information or support by using the two-page Request for Body of Knowledge Information or Support form illustrated in figure 4. The first page of this form indicates all necessary IST or POST approvals for requesting the needed BOK information or support. The second page defines the actual request. Use of this form provides a record of all key information exchanges across firewalls. When such a request form is no longer needed, the BOK member of whom the request was made must either shred or burn the document to avoid inadvertent disclosure of protected information.

REQUEST FOR BODY OF KNOWLEDGE INFORMATION OR SUPPORT

This is an Industry Support Team (IST) request for information or support from a Body of Knowledge (BOK) member.

IST Name: _____

Industry Partner: _____

To ensure proper handling and transfer of the requested information, please initial as indicated below.

Review and concur with request:

IST Leader: _____ Date _____

Accept request for information or support and agree to information protection procedures:

BOK Member: _____ Date _____

Accept information or support deliverable from BOK:

IST Leader: _____ Date _____

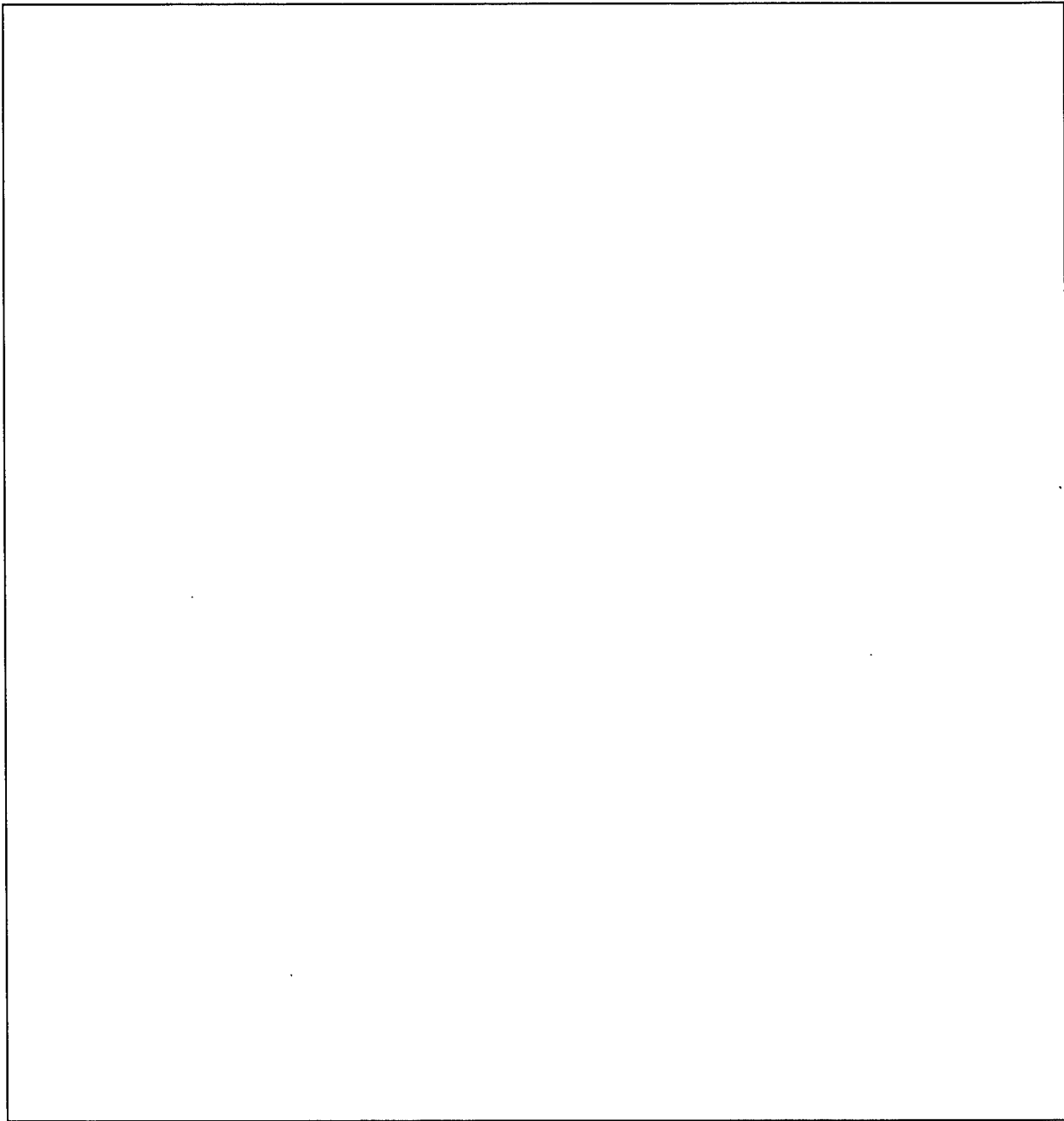
Transfer of deliverable to industry (if applicable):

IST Leader: _____ Date _____

Page 1 of 2

Figure 4. Request for Body of Knowledge Information or Support.

Description of information or support requested:



IST Request Originator: _____

Date: _____

Page 2 of 2

Figure 4. Request for Body of Knowledge Information or Support (contd).

2.4.5 Termination of Team Membership or Team Support

When an employee terminates membership or support to an IST, the ILPOC is responsible for ensuring that the employee is provided an exit briefing. The exit briefing will be used to explain any remaining obligations of the employee for protection of competition-sensitive information and to discuss eligibility for future IST membership, etc. The individual will acknowledge understanding these responsibilities and restrictions by signing an exit briefing form. Figure 5 is a sample exit briefing form.

EXIT BRIEFING FOR TERMINATION OF TEAM MEMBERSHIP OR SUPPORT

1. I was assigned to a particular Industry Team or provided support to Industry Teams. At this time, I am no longer part of the team or providing assistance to the teams.
2. I understand that although I am no longer assisting an Industry Team, I am still obligated to protect competition-sensitive and company-proprietary information as required by the Non-Disclosure Agreement I signed.
3. **I understand that my duty to protect all proprietary information I have obtained from an Industry Team will exist even after there is an award or down-select of one of the Industry Teams.**
4. If I was assigned to a specific Industry Team that was in competition with another Industry Team, I understand that until there is a down-select between the Industry Teams, I will still have the following duties:
 - a. I will protect all competition-sensitive information. I also understand that the competition-sensitive information is to be used only for SSC San Diego performance of the Agreement with the Industry Team. All competition files should be returned to the Industry Teams or destroyed. **Note: Some competition-sensitive information is also considered company-proprietary information and thus will still require protection after a down-select of the Industry Teams.** Thus, prior to any release of this information, I will consult with the Industry Liaison Point of Contact to determine whether any information will remain protected.
 - b. I will not work for the competing Industry Team until after there is a down-select of the Industry Teams. Prior to working for a competing Industry Team, I will contact the Office of Counsel to obtain a legal opinion.
5. I will coordinate with the Industry Liaison Point of Contact to ensure my badge is changed to properly reflect that I am no longer assigned to or supporting a particular Industry Team.

If I have any questions as to my duties or obligations to protect information, I will contact the Office of Counsel at (619) 553-4703.

Project Name

Printed Name

Date

Signature

Figure 5. Exit Briefing for Termination of Team Membership or Support.

3. ROLES AND RESPONSIBILITIES

Key roles and responsibilities are defined herein to provide direct support to the Industry concerns and to maintain acquisition integrity at all times. To this end, the following roles and their associated responsibilities are provided.

3.1 BUSINESS DEVELOPMENT OFFICE INDUSTRY LIAISON POINT OF CONTACT

The Business Development Office (BDO) functions as the Industry Liaison Point of Contact (ILPOC) for SSC San Diego's work for Industry activities. In this capacity, the BDO acts as the liaison between Industry seeking SSC San Diego technical services and any component of the SSC San Diego organization. Any understanding or agreement to provide technical services by SSC San Diego to Industry without the assistance of the ILPOC and/or formal Command approval for the initiation of work between SSC San Diego personnel and Industry is prohibited.

The ILPOC has the following responsibilities:

- ❑ Provide information protection briefings to all SSC San Diego employees involved in a Work for Industry Agreement. Keep records of all employees who have participated in such briefings.
- ❑ Initiate special badge requests for all SSC San Diego employees involved in a Work for Industry Agreement who require such identification.
- ❑ Ensure that Industry's proprietary information is protected pursuant to the requirements of this document.
- ❑ Obtain signed Non-Disclosure Agreements (NDAs) from all IST and BOK members.
- ❑ Maintain records of and provide status on all SSC San Diego IST and BOK members.
- ❑ Ensure that IST members leaving a team receive an exit briefing.
- ❑ Alert any appropriate personnel and SSC San Diego management concerning any issues regarding the proper protection of information or failure of such protection.

3.2 OFFICE OF COUNSEL

The Office of Counsel acts as the legal advisor for all Work for Industry Agreements. The Office actively works with all involved parties to assure legal compliance with all statutory requirements.

The Office of Counsel has the following responsibilities:

- ❑ Ensure SSC San Diego's and Industry's work and information is firewalled to protect information and acquisition integrity.
- ❑ Maintain original agreements and ensure all files are properly secured.
- ❑ Attend and provide legal advice during all Work for Industry information protection briefings to ensure compliance with this document and the appropriate Standard Operating Procedure (SOP).
- ❑ Use results generated in response to an Industry request strictly for that original demand. The same results shall not be used to respond to any other Industry inquiry.
- ❑ Provide confidential legal advice regarding information protection to all SSC San Diego employees involved in Work for Industry Agreements.

3.3 CONTRACTS

Contracts Division personnel serve as the liaison between SSC San Diego and Industry in the negotiation and completion of all contract-related paperwork involved in an agreement with Industry.

The Contracts Division personnel will be responsible for information protection pursuant to the Guidelines for Information Protection under Work for Industry Agreements.

- ☐ Information gained by Contracts personnel that is acquisition-sensitive must be kept in confidence.

3.4 SECURITY

Security personnel will act as the primary liaison between SSC San Diego and Industry to assure that all required security measures are in place and all required security paperwork is completed prior to executing an agreement with Industry.

Security personnel will have the following responsibilities:

- ☐ Ensure timely processing of Industry's incoming Visit Authorization Letters (VALs).
- ☐ Issue special picture badges to IST members and appropriate Industry employees.
- ☐ Review the Division of Defense Contract Security Classification Specification, DD 254, received from Industry and included with the agreement.
- ☐ Assist the IST Leader in obtaining the required Industry classification guides for information protection.
- ☐ Ensure protection of all information systems to include the protection against unauthorized access to, or modification of, information via computer.
- ☐ Act as liaison with the Purchaser's security office. The Security Contracting Officer's Representative (COR) will be the primary point of contact for security matters with Industry.

3.5 SSC SAN DIEGO INDUSTRY SUPPORT TEAM LEADERS

An individual designated as the IST Leader will provide technical and administrative leadership for each IST. The IST Leader ensures that the tasking is executed. This may include execution of portions of the task by the IST Leader. In the event that execution of a particular task is performed exclusively by BOK members, no IST will be formed or IST Leader assigned, and all responsibilities normally performed by an IST Leader will be assumed by the ILPOC.

The SSC San Diego IST Leader will have the following responsibilities:

- ☐ Ensure that all IST members are properly briefed on information protection procedures and have received a copy of this document.
- ☐ Provide cover sheets and magnetic media labels to team members (see Appendix B, Attachments 1 and 2).
- ☐ Ensure all team members have signed the appropriate NDA. Ensure that all team members obtain signed NDAs from members in the technical BOK who receive information from the IST member.
- ☐ Ensure the release of technical information to BOK members is the minimum required to accomplish the requested tasking. Employ procedures to minimize release of any unauthorized information to BOK members by the IST.
- ☐ Concur with requests by IST members for interactive data environment (IDE) access.

- ❑ Identify and communicate IST staffing and resource needs via the Division, Business, and/or Operations Deputies, or the ILPOC, as appropriate. Alert any applicable personnel and the ILPOC concerning any issues regarding the proper protection of information.

3.6 INDUSTRY SUPPORT TEAM MEMBER

An IST member is a recognized subject matter expert for a specific project or initiative that applies to the program. This individual is selected to be part of an IST but can only support one Industry concern on each project. The IST members are the principal executors of tasking received from Industry. In this capacity, they may address technical issues themselves or, if additional expertise is required, they can make inquiries of or enlist BOK members to assist in task execution.

IST participants have the following responsibilities:

- ❑ Adhere to the requirements of this document and the appropriate SOP governing the employee's work for Industry.
- ❑ Ensure that no source-selection information is available to the IST members.
- ❑ Report any inadvertent disclosures of protected information to the IST Leader and/or the ILPOC and Office of Counsel.

3.7 BODY OF KNOWLEDGE MEMBERS

A BOK member is a recognized subject matter expert for a specific project or initiative that applies to the program. The BOK also includes administrative personnel such as the ILPOC, Office of Counsel, and Contracts Department support. Unlike the IST participants, BOK members' unique qualifications and/or availability prevent exclusive availability to a single Industry concern. BOK members' technical services can be requested by IST or POST members in accordance with the procedures specified in this document. When tasked to support an IST or POST, the BOK member will adhere to the same information protection guidelines as IST and POST members.

BOK members have the following responsibilities:

- ❑ Execute technical tasking as provided by an IST or POST member. Release technical products and deliverables only to the requesting IST or POST member or Leader.
- ❑ Adhere to the procedures outlined in this document and the appropriate SOP.

3.8 PROGRAM OFFICE SUPPORT TEAM MEMBERS

SSC San Diego technical and support personnel may be funded and tasked to provide direct support at the government Program Office level as a member of a Program Office Support Team (POST). In this capacity, those SSC San Diego employees who are POST members function as an extension of the Program Office and may have access to information from competing teams for technical evaluations and source-selection recommendations. POST members must ensure that they refrain from exchanging information with IST and BOK members unless authorized to do so as a requirement of their assigned POST responsibilities.

POST members have the following responsibilities:

- ❑ Provide direct technical and administrative support to the sponsoring Program Office.
- ❑ Assist Program Office personnel in performing evaluations, trade-offs, and source-selection recommendations and other studies and analyses as requested.

4. SECURITY

In support of the security requirements outlined in this section, processes are required for handling materials received from Industry or generated by the IST. Specifically, the following paragraphs document the use of cover sheets, magnetic media labels, and unique badges, as well as information security, classification management, physical security, classified visitation, and destruction of material.

4.1 COVER SHEETS

To facilitate proper Operational Security (OPSEC) and physical security, each SSC San Diego participant shall be provided with unique cover sheets. These sheets shall be used to protect written or printed material at all times. If the material is also classified, the appropriate red for Secret and blue for Confidential Standard Form (SF 704 or SF 705) cover sheet will be used as the topmost sheet. Attachment 1 in Appendix B is a sample cover sheet to be used for each IST. The cover sheets will be provided by the IST Leader at the time of firewalling. Additional copies will be available through the SSC San Diego IST Leaders.

4.2 MAGNETIC MEDIA LABELS

To facilitate proper OPSEC, physical security, and information security (INFOSEC), each SSC San Diego participant shall provide proper handling of all Industry and IST associated magnetic media. To this end, each SSC San Diego IST will be provided with magnetic media labels unique to each IST. In addition to the standard labels required to denote the overall security classification of the media, these IST-specific labels shall be placed on all removable and fixed magnetic memory used in support of direct work for Industry. Attachment 2 in Appendix B illustrates samples of magnetic media labels for both classified and unclassified media.

4.3 BADGES FOR SSC SAN DIEGO IST MEMBERS

To facilitate proper OPSEC and physical security, each SSC San Diego IST and POST participant will be issued and required to wear an SSC San Diego IST badge that uniquely identifies his/her participation in a Work for Industry program. (See Attachment 3 in Appendix B). The badges will encompass the existing SSC San Diego employee badge and include additional descriptive wording identifying the particular Industry concern to which the SSC San Diego employee is assigned. Only after the employee acknowledges that he/she received a briefing regarding firewalls and information protection and has signed and submitted the appropriate NDA will the IST Leaders request the picture identification badges be issued for the length of the Agreement. The badge shall be worn throughout the specific period of performance. If there are several phases to the Program, the termination date of the badges may be extended as needed. Identification badges are the property of the U.S. Government and will be worn and used for official business only. Unauthorized use of an SSC San Diego badge by Industry personnel will be reported to the Defense Security Service (DSS); such use by an SSC San Diego employee will be reported to the Security Office. Identification badges must be worn in plain sight at all times while on the SSC San Diego base.

4.4 INFORMATION SECURITY

In the event Industry provides information to SSC San Diego that is other than proprietary or competition-sensitive, Industry will provide guidance for the protection of any special information (classified, unclassified) associated with the project, test articles, technical information, test data, specifications, etc. If classified information must be processed, the Information Systems to be used

for such processing must be locally approved to operate for the highest classification level of information, and users must comply with applicable policies. In the absence of specific markings to the contrary or if instructional guidance or declarations are missing, SSC San Diego will assume no protection is required other than that outlined in this document for protection of proprietary and/or competition-sensitive information.

4.5 CLASSIFICATION MANAGEMENT

If project-related information is classified, Industry shall provide the necessary classification guidance and security requirements on the Department of Defense Contract Security Classification Specification (DD 254) to SSC San Diego prior to commencing work. The test article and data developed as a result of testing will be handled in accordance with SECNAVINST 5510.36, Department of the Navy (DON) Information Security Program (ISP) Regulation for safeguarding such articles or information against unauthorized disclosure.

4.6 PHYSICAL SECURITY

When working on SSC San Diego property pursuant to the Agreement, Industry and IST members will comply with all emergency rules and procedures established at SSC San Diego. These SSC San Diego regulations include, but are not limited to, physical security requirements for personnel, material, and vehicle access.

4.6.1 Physical Security Procedures

SSC San Diego will act to protect against any breach in physical security by engaging the services of a roving patrol force. SSC San Diego, or other Government security forces, will respond to any physical breach of security pursuant to applicable instructions and procedures including, but not limited to, physical checks of the window or door access points, classified containers, and locating any improperly secured documents or spaces.

4.6.2 Vehicle Inspection

All SSC San Diego and contractor personnel are subject to random inspections of their person, vehicles, and personal items. Consent to these inspections is implied when personnel accept either a badge or a vehicle pass/decal permitting entrance to this Command.

4.7 VISIT AUTHORIZATION LETTER

Prior to an Industry-concern employee's classified access to SSC San Diego's property, the employee must submit a Visit Authorization Letter (VAL). Submission of a valid VAL is the responsibility of Industry.

All VALs will be prepared in accordance with the National Industrial Security Program, Operating Manual (NISPOM) DoD 5220.22-M. The VAL should be sent to the Commanding Officer, ATTN Code D03541, SSC San Diego, 49275 Electron Drive, San Diego, CA 92152-5001. Facsimile requests will be accepted at (619) 553-6169 and verified on 553-3203.

VALs must be received at least 1 week prior to the expected arrival of the visitor to ensure necessary processing of the request.

Following receipt of an accepted VAL, the SSC San Diego ID/Access and Administrative Services, D03541, will issue temporary identification badges to the Industry employee. The IST Leader for the responsible Program will request issuance of program appropriate badges for Industry employees. Unauthorized use of an SSC San Diego badge by Industry personnel will be reported to

the Defense Security Service; such use by SSC San Diego personnel will be reported to the Security Office. Identification badges must be worn in plain sight at all times while at this Command.

4.8 DESTRUCTION OF MATERIAL

All classified, unclassified, competition-sensitive, company-proprietary, or source-selection information must be properly destroyed when it is no longer needed. When destroying any material, all personnel at SSC San Diego will follow the directions contained in the Classified Material Control Center (CMCC) Handbook, SD 031, Rev. 1,

<http://iweb.nosc.mil/services/sti/publications/pubs/sd/031/sd031.pdf> or

<http://iweb.nosc.mil/services/sti/publications/pubs/sd/031/index.html>.

5. CONTACT WITH PARTIES OTHER THAN THE INDUSTRY CONCERN WITH WHICH SSC SAN DIEGO IS WORKING

5.1 PROCEDURES

In the event an Industry subcontractor approaches an SSC San Diego employee requesting the services of SSC San Diego, the employee should report the contact to the ILPOC and the appropriate IST Leader. For example, if an XYZ, Inc., subcontractor on the PQR contract approached SSC San Diego to work for it in the performance of its subcontract to XYZ, Inc., the SSC San Diego employee approached must inform the ILPOC of the contact.

The ILPOC will first confer with Contracts and the Office of Counsel to make a determination regarding whether the requested work fits under the scope of the existing agreement with the program's prime contractor. If a determination is made that the work is within the scope of the existing agreement, the ILPOC will contact the requestor and refer him/her to the IST Leader for consultation.

If it is determined that the work is not within the scope of the existing agreement, a modification to the existing agreement or a new agreement between SSC San Diego and the requestor must be made. Prior to entering into any additional agreements with Industry, the following determinations must be made:

- ☐ Whether the IST Leader believes there is any perceived conflict of interest in performing the work.
- ☐ Whether there is any internal conflict of interest. This determination will be made with the assistance of the Office of Counsel.
- ☐ If there is a perceived conflict of interest or violation of firewall protection, the ILPOC will determine whether those conflicts or violations can be overcome to protect all interested parties and information.

If the ILPOC determines that the work can proceed, the ILPOC will ensure that all appropriate firewalls and information protection requirements are in place pursuant to this document.

APPENDIX A: DEFINITIONS

Agreement: The Sale of Articles or Services Agreements between Industry concerns and SSC San Diego pursuant to 10 U.S.C. 2553.

Body of Knowledge (BOK): SSC San Diego employees who have either technical recognized subject matter expertise or administrative responsibilities. Technical BOK members include all engineers, scientists, or other subject matter specialists that have unique expertise in a particular scientific area. Administrative BOK members include the Business Development Office Industry Liaison Points of Contact, other Business Development Office personnel, Contracts Division personnel, Office of Counsel and its office support personnel, Security Office personnel, and any other non-technical support necessary to carry out the requirements of the Industry program.

Company Proprietary: Material and information relating to or associated with a company's products, business, or activities, including but not limited to: financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; process; and know-how that have been clearly identified and properly marked as proprietary information, trade secrets, or company confidential information.

Competing Industry Concerns: Any two or more Industry concerns in competition on a single program.

Competition-Sensitive Information: Information in any form, whether written or otherwise, that discloses, in whole or in part, information with respect to work performed, planned to be proposed, or actually proposed by either Industry concern and that can reasonably be expected to have a material effect on the competitive position of such Industry concern in competing with the other Industry concern. This information must also be either (1) appropriately labeled "Competition-Sensitive Information" or (2) oral or visual information that is verbally designated at the time of disclosure as "Competition-Sensitive Information" and subsequently confirmed as such within 30 days after the initial oral or visual disclosure in written documentation, marked as "Competition-Sensitive Information" and listing or summarizing the oral or visual information that is disclosed as Competition-Sensitive. In addition, Competition-Sensitive Information includes information that is derived by the receiving party from information designated as "Competition-Sensitive Information" by the providing party. Notwithstanding the above, information will not be considered Competition-Sensitive Information to the extent, if any, that it (1) is in the public domain or becomes generally available to the public through no contractual breach; (2) is received by any member of an Industry concern from a third party free to disclose such information; or (3) was developed independently by the competing Industry concern receiving the "Competition-Sensitive Information" prior to that competing Industry concern's receipt of such information. NOTE: This does not include source-selection information.

For Official Use Only (FOUO): This term is not a security classification. The term governs the control and protection of all unclassified information, records, and other materials that are exempt from general public disclosure and indiscriminate handling because of significant and legitimate Governmental reasons, under Freedom of Information Act (FOIA).

Firewall: A physical or conceptual separation of individuals working in the same organization to prevent disclosure or transfusion of sensitive or proprietary information from one person or group to another, within the same organization. An example of the necessity of a firewall is when SSC San Diego is working with different Industry concerns in competition with each other for the same contract award.

Industry Support Team (IST): SSC San Diego personnel assigned to work on an Industry project for one Industry concern. The Industry concern may or may not be in a competitive situation.

Information: Encompasses company-proprietary information, competition-sensitive information, and source-selection information.

Information Security: The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Invention: Any invention or discovery that is or may be patentable under Title 35 of the United States Code.

Non-Disclosure Agreement (NDA): An agreement to protect competition-sensitive, company-proprietary, and source-selection information from disclosure to unauthorized personnel. Within these Guidelines there are two types of NDAs, one for the IST and one for the BOK members (figures 2 and 3).

Operational Security: A systematic and proven process by which the U.S. Government and its supporting contractors (or other activity/organization) can deny information to potential adversaries about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government (or other) activities.

Party: An Industry concern or SSC San Diego.

Physical Security: The process of deterring or preventing sabotage, terrorist, or dissident activity, theft, or misappropriation of Government property and other criminal or unauthorized acts (preventing, reducing, or deterring the incidence of crime of opportunity).

Program Office Support Team (POST): SSC San Diego personnel who receive tasking and funding from a government Program Office. POST members function as an extension of the Program Office and have the same information protection requirements as Program Office personnel.

Source-Selection Information: Information that is prepared for use by a Federal agency for the purpose of evaluating a bid or proposal to enter into a Federal agency procurement contract, if that information has not been previously made available to the public or disclosed publicly. Source-selection information includes, but is not limited to, the following information:

- ☐ Proposed costs or prices submitted in response to a Federal agency solicitation, or lists of those proposed costs or prices
- ☐ Source-selection plans
- ☐ Technical evaluation plans
- ☐ Technical evaluations of proposals
- ☐ Cost or price evaluations of proposals
- ☐ Competitive range determinations that identify proposals that have a reasonable chance of being selected for award of a contract
- ☐ Rankings of bids, proposals, or competitors
- ☐ Reports and evaluations of source-selection panels, boards, or advisory councils
- ☐ Other information based on a case-by-case determination by the head of the agency or designee, or the contracting officer, that its disclosure would jeopardize the integrity or successful completion of the Federal agency procurement to which the information relates

SSC San Diego: Space and Naval Warfare Systems Center, San Diego, located at 53560 Hull Street, San Diego, CA 92152-5001.

Subject Data: All data first produced in the performance of work under the agreement between Industry and SSC San Diego.

Subject Invention: Any invention made in the performance of work under the agreement between Industry and SSC San Diego.

APPENDIX B: ATTACHMENTS

Attachment 1. Sample cover sheet.

PROGRAM NAME

COMPETITION-SENSITIVE OR COMPANY-PROPRIETARY INFORMATION

THIS IS A COVER SHEET FOR COMPETITION-SENSITIVE OR COMPANY-PROPRIETARY INFORMATION.

**ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO
PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE
_____ PROGRAM.**

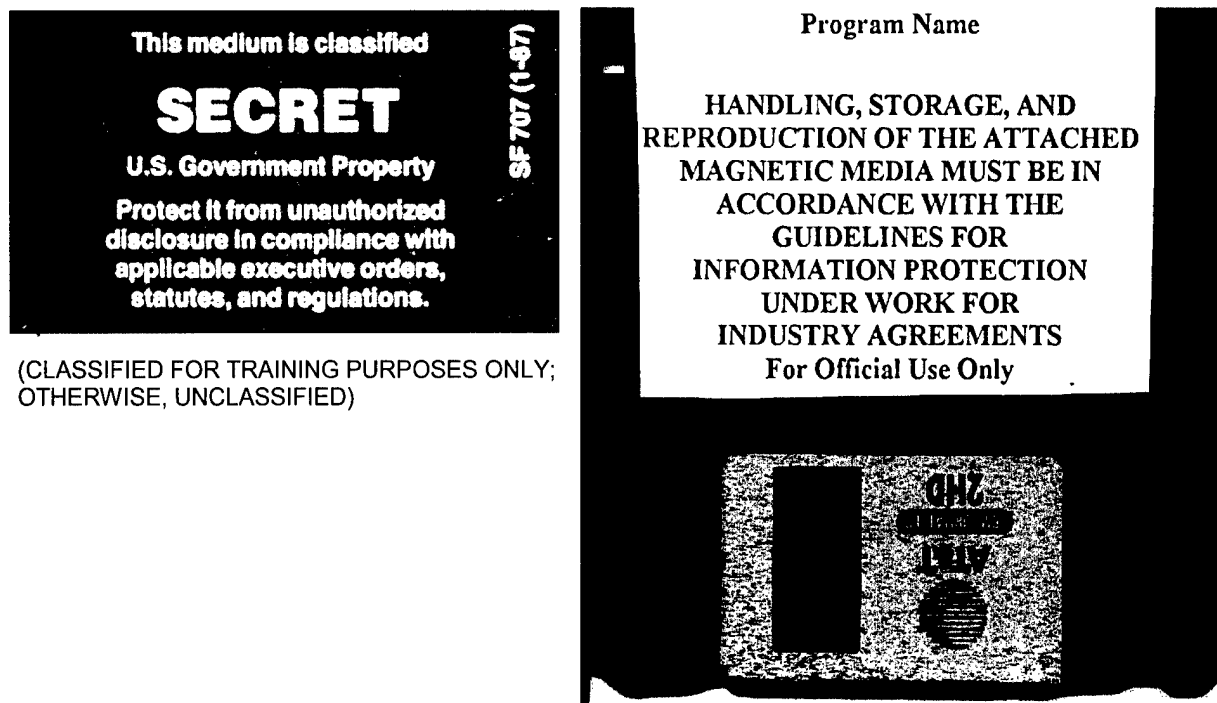
**HANDLING, STORAGE, REPRODUCTION, AND DISPOSITION OF THE
ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE
EXECUTIVE ORDER(S), STATUTE(S), AND AGENCY IMPLEMENTING
REGULATIONS.**

**(THIS COVER SHEET IS UNCLASSIFIED)
FOR OFFICIAL USE ONLY**

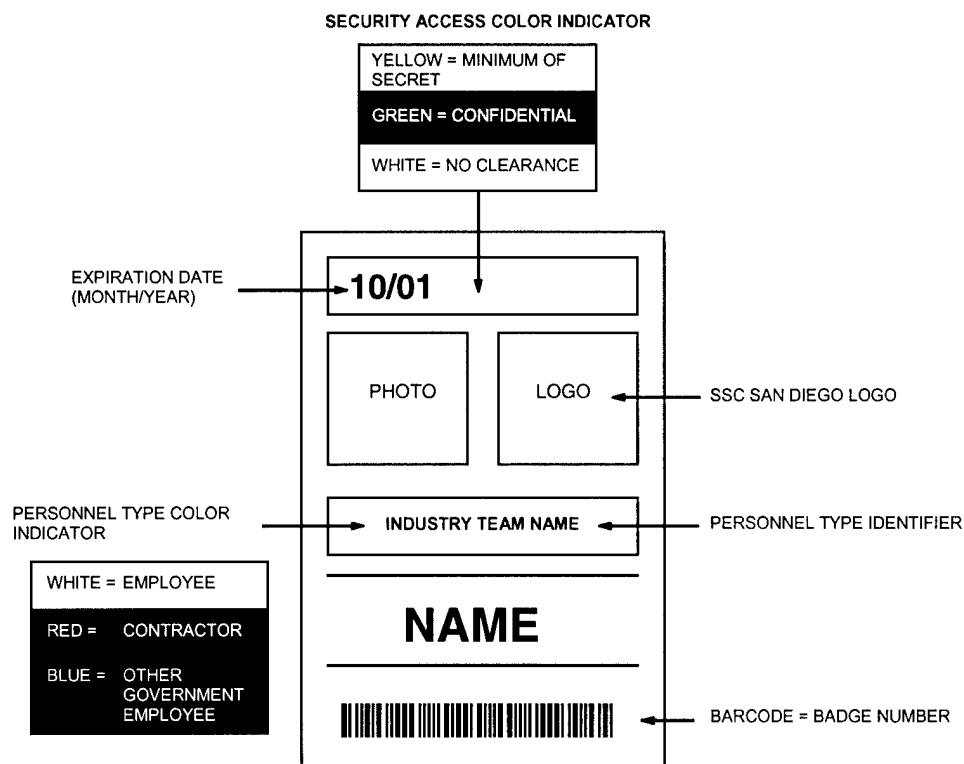
PROGRAM NAME

COMPETITION-SENSITIVE OR COMPANY-PROPRIETARY INFORMATION

Attachment 2. Magnetic media labels.



Attachment 3. SSC San Diego badge information.



| REPORT DOCUMENTATION PAGE | | | | | Form Approved OMB No. 0704-01-0188 | |
|--|-------------|-------------------------|-------------------------------|--|---|--|
| The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. | | | | | | |
| PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS. | | | | | | |
| 1. REPORT DATE (DD-MM-YYYY) 02-2000 | | 2. REPORT TYPE Final | | | 3. DATES COVERED (From - To) | |
| 4. TITLE AND SUBTITLE GUIDELINES FOR INFORMATION PROTECTION UNDER WORK FOR INDUSTRY AGREEMENTS | | | | 5a. CONTRACT NUMBER | | |
| | | | | 5b. GRANT NUMBER | | |
| | | | | 5c. PROGRAM ELEMENT NUMBER | | |
| 6. AUTHORS J. A. Roese, C. L. Concha, F. L. Esaias, R. E. Fox, C. P. Kneib, J. Mansfield, J. L. Miller-Corona, J. V. Simmons, P. Talley, J. A. McKamey, and J. G. Wester | | | | 5d. PROJECT NUMBER | | |
| | | | | 5e. TASK NUMBER | | |
| | | | | 5f. WORK UNIT NUMBER | | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) SSC San Diego San Diego, CA 92152-5001 | | | | 8. PERFORMING ORGANIZATION REPORT NUMBER TD 3099 | | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | | | | 10. SPONSOR/MONITOR'S ACRONYM(S) | | |
| | | | | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) | | |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited. | | | | | | |
| 13. SUPPLEMENTARY NOTES | | | | | | |
| 14. ABSTRACT This document is meant to ensure acquisition integrity for the SSC San Diego Work for Industry Agreements established with Industry pursuant to the authority in Title 10 U.S. Code, Section 2553 (Sale of Articles of Services to Industry), 2539b (Availability of Government Testing Facilities and Sale of Information to Industry), 2371 (Research Projects: Transactions Other Than Contracts and Grants), and Title 15 U.S. Code, Section 3710a (Cooperative Research and Development Agreements). | | | | | | |
| 15. SUBJECT TERMS Information protection Work for Industry Agreements Title 10 U.S. Code, Sections 2553 and 2539b Title 15 U.S. Code, Section 3710a | | | | | | |
| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON | |
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | John A. Roese | |
| U | U | U | UU | 38 | 19b. TELEPHONE NUMBER (Include area code) (619) 553-1166 | |

INITIAL DISTRIBUTION

| | | |
|-------------------------------------|----------------|-------|
| D0012 | Patent Counsel | (1) |
| D0271 | Archive/Stock | (6) |
| D0274 | Library | (2) |
| D027 | M. E. Cathcart | (1) |
| D0271 | D. Richter | (1) |
| D11 | J. A. Roese | (120) |
| Internal Distribution List B (1 ea) | | (60) |

Defense Technical Information Center
Fort Belvoir, VA 22060-6218 (4)

SSC San Diego Liaison Office
C/O PEO-SCS
Arlington, VA 22202-4804

Center for Naval Analyses
Alexandria, VA 22302-0268

Navy Acquisition, Research and Development
Information Center
Arlington, VA 22202-3734

Government-Industry Data Exchange Program
Operations Center
Corona, CA 91718-8000